The US-CERT Cyber Security Bulletin provides a summary of new and updated vulnerabilities, exploits, trends, and malicious code that have recently been openly reported. Information in the Cyber Security Bulletin is a compilation of open source and US-CERT vulnerability information. As such, the Cyber Security Bulletin includes information published by sources outside of US-CERT and *should **not** be considered the result of US-CERT analysis or as an official report of US-CERT*. Although this information does reflect open source reports, it is not an official description and should be used for informational purposes only. The intention of the Cyber Security Bulletin is to serve as a comprehensive directory of pertinent vulnerability reports, providing brief summaries and additional sources for further investigation.

Vulnerabilities

- Windows Operating Systems
  - eStara Softphone Multiple Denial of Service
  - GA's Forum SQL Injection
  - HP Insight Manager Arbitrary File Access
  - HP PSC 1210 All-in-One Drivers Unspecified Vulnerability
  - Microsoft HTML Help Workshop Arbitrary Code Execution
  - Microsoft Internet Explorer Arbitrary Code Execution
  - Microsoft PowerPoint 2000 Information Disclosure
  - Microsoft Windows IGMPv3 Denial of Service
  - Microsoft Windows Korean Input Method Editor Privilege Elevation
  - Microsoft Windows Media Player Arbitrary Code Execution
  - Microsoft Windows Media Player Arbitrary Code Execution
  - Microsoft Windows Web Client Arbitrary Code Execution
  - Mirabilis ICQ Arbitrary Code Execution
  - Winamp Arbitrary Code Execution
  - Whomp Real Estate Manager XP 2005 SQL Injection
  - **WebWasher Security Bypassing (Updated)**
- Unix/ Linux Operating Systems
  - Apple Mac OS X Undocumented System Call Denial of Service
  - DataparkSearch Engine Cross-Site Scripting
  - DocMGR Remote File Include
  - GnuPG Detached Signature Verification Bypass
  - Honeyd IP Reassembly Remote Virtual Host Detection
  - **Horde Kronolith HTML Injection (Updated)**
  - IBM AIX Denial of Service
  - IBM AIX ARP Buffer Overflow
  - **ImageMagick Utilities Image Filename Remote Command Execution (Updated)**
  - Isode M-Vault Server LDAP
  - **libpng Buffer Overflow (Updated)**
  - **Multiple Vendors Linux Kernel Integer Overflow (Updated)**
  - **Multiple Vendors OpenSSH SCP Shell Command Execution (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel ICMP Error Handling Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Vulnerabilities (Updated)**
  - Multiple Vendors Linux Kernel NFS ACL Access Control Bypass
  - **Multiple Vendors Linux Kernel ProcFS Kernel Memory Disclosure (Updated)**
  - Multiple Vendors Noweb Insecure Temporary File Creation
  - **Multiple Vendors Linux Kernel 'mq_open' System Call Denial of Service (Updated)**
  - Multiple Vendors GnuTLS libtasn1 DER Decoding Remote Denial of Service
  - NeoMail Security Bypass
  - PAM-MySQL SQL Logging & Double-Free
  - PowerD Remote Format String
  - PyBlosxom Information Disclosure
  - **Heimdal RSHD Server Elevated Privileges (Updated)**
  - **scponly Privilege Escalation & Security Bypass (Updated)**
  - Siteframe Beaumont Cross-Site Scripting
  - Sun Solaris 'in.rexecd' Elevated Privileges
  - **SUSE NFS-SERVER Remote Buffer Overflow (Updated)**
  - SUSE LD Insecure RPATH / RUNPATH Arbitrary Code Execution
  - Virtual Hosting Control System Multiple Input Validation & Access Validation
- Multiple Operating Systems
  - 2200net Calendar System SQL Injection
  - Ansilove File Disclosure & File Upload
  - **CRE Loaded Files.PHP Access Validation (Updated)**
  - Cisco Multiple Products TACACS+ Authentication Bypass
  - Clever Copy HTML Injection
  - **ContentServ SQL Injection (Updated)**
  - CPAINT Cross-Site Scripting
  - CPG Dragonfly File Include
  - QwikiWiki Cross-Site Scripting
  - DeltaScripts PHP Classifieds SQL Injection
  - Dotproject File Include & Information Disclosure
  - e107 BBCode HTML Injection
  - FarsiNews Directory Traversal & File Include
  - FortiGate URL Filter & Virus Scanning Bypass
  - PHPNuke Cross-Site Scripting
  - Hinton Design PHPHD Multiple Input Validation & Authentication Bypass
  - Hinton Design phpht Topsites Input Validation
  - Hinton Design PHPStatus Multiple Input Validation
  - Hitachi Business Logic Cross-Site Scripting & SQL Injection
  - HiveMail Multiple Vulnerabilities
  - IBM Lotus Domino iNotes Multiple HTML & Script Injection
  - IBM Tivoli Directory Server LDAP Denial of Service
  - IBM Lotus Notes Multiple Vulnerabilities
  - ImageVue Multiple Vulnerabilities
  - Invision Power Board User Registration Remote Denial of Service

---

Vulnerabilities

The tables below summarize vulnerabilities that have been reported by various open source organizations or presented in newsgroups and on web sites. **Items in bold designate updates that have been made to past entries.** Entries are grouped by the operating system on which the reported software operates, and vulnerabilities which affect both Windows and Unix/ Linux Operating Systems are included in the Multiple Operating Systems table. *Note*, entries in each table are not necessarily vulnerabilities *in* that operating system, but vulnerabilities in software which operate on some version of that operating system.

Entries may contain additional US-CERT sponsored information, including Common Vulnerabilities and Exposures (CVE) numbers, National Vulnerability Database (NVD) links, Common Vulnerability Scoring System (CVSS) values, Open Vulnerability and Assessment Language (OVAL) definitions, or links to US-CERT Vulnerability Notes. Metrics, values, and information included in the Cyber Security Bulletin which has been provided by other US-CERT sponsored programs, is prepared, managed, and contributed by those respective programs. CVSS values are managed and provided by the US-CERT/ NIST National Vulnerability Database. Links are also provided to patches and workarounds that have been provided by the product's vendor.

The Risk levels are defined below:

High - Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

Medium - Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.

Low - Vulnerabilities will be labeled "Low" severity if they have a CVSS base score of 0.0-3.9.

Note that scores provided prior to 11/9/2005 are approximated from only partially available CVSS metric data. Such scores are marked as "Approximated" within NVD. In particular, the following CVSS metrics are only partially available for these vulnerabilities and NVD assumes certain values based on an approximation algorithm: AccessComplexity, Authentication, ConfImpact of 'partial', IntegImpact of 'partial', AvailImpact of 'partial', and the impact biases.

Windows Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources

eStara Softphone 3.0.1.14, 3.0.1.46, 3.0.1.47	Multiple vulnerabilities have been reported in Smartphone that could let remote malicious users to cause a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	eStara Softphone Multiple Denial of Service	Not Available	Security Focus, ID: 16629, February 14, 2006
GAsoft GA's Forum	An input validation vulnerability has been reported in GA's Forum that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GA's Forum SQL Injection CVE-2006-0669	7	Security Tracker, Alert ID: 1015600, February 8, 2006
HP Insight Manager 4.2, 4.2 SP1, 4.2 SP2, 5.0, 5.0 SP1, 5.0 SP2, and 5.0 SP3	A Directory Traversal vulnerability has been reported in Insight Manager that could let remote malicious users obtain arbitrary file access. HP Solution Currently we are not aware of any exploits for this vulnerability.	HP Insight Manager Arbitrary File Access CVE-2005-2006	3.3	Security Tracker, Alert ID: 1015605, February 9, 2006
HP PSC 1210 All-in-One Drivers	An unspecified vulnerability has been reported in PSC 1210 All-in-One Drivers. Upgrade to version 1.0.06 Currently we are not aware of any exploits for this vulnerability.	HP PSC 1210 All-in-One Drivers Unspecified Vulnerability CVE-2006-0672	4.9	Secunia, Advisory: SA18770, February 10, 2006
Microsoft HTML Help Workshop 4.74.8702.0	A buffer overflow vulnerability has been reported in HTML Help Workshop that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. **An exploit script, htmlws.c, has been published.**	Microsoft HTML Help Workshop Arbitrary Code Execution CVE-2006-0564	7	Secunia, Advisory: SA18740, February 6, 2006 **US-CERT VU#124460**
Microsoft Internet Explorer 5.0.1 SP4	A vulnerability has been reported in Internet Explorer, WMF image parsing, that could let remote malicious users to execute arbitrary code. Microsoft Currently we are not aware of any exploits for this vulnerability.	Microsoft Internet Explorer Arbitrary Code Execution CVE-2006-0020	7	Microsoft, Security Bulletin MS06-004, February 14, 2006 Technical Cyber Security Alert TA06-045A Cyber Security Alert SA06-045A US-CERT VU#839284
Microsoft Internet Explorer various versions	A vulnerability has been reported in Internet Explorer that could let remote malicious users to execute arbitrary code. Microsoft Currently we are not aware of any exploits for this vulnerability.	Internet Explorer Arbitrary Code Execution CVE-2006-0020	7	Microsoft, Security Advisory 913333, February 7, 2006 Technical Cyber Security Alert TA06-045A Cyber Security Alert SA06-045A **US-CERT VU#312956**
Microsoft PowerPoint 2000 SP3	A vulnerability has been reported in PowerPoint 2000 that could let remote malicious users disclose information. Microsoft Currently we are not aware of	Microsoft PowerPoint 2000 Information Disclosure CVE-2006-0004	Not Available	Microsoft, Security Bulletin MS06-010, February 14, 2006 US-CERT VU#963628

	any exploits for this vulnerability.			
Microsoft Windows IGMPv3 XP and Server 2003 various versions	A vulnerability has been reported in Windows IGMPv3 that could let remote malicious users cause a Denial of Service. Microsoft There is no exploit code required.	Microsoft Windows IGMPv3 Denial of Service CVE-2006-0021	Not Available	Microsoft, Security Bulletin MS06-007 V1.1, February 14, 2006
Microsoft Windows Korean Input Method Editor XP, Server 2003, and Office 2003 various versions	A vulnerability has been reported in WIndows Korean Input Method Editor that could let local malicious users obtain elevated privileges. Microsoft Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Korean Input Method Editor Privilege Elevation CVE-2006-0008	Not Available	Microsoft, Security Bulletin MS06-009, February 14, 2006 US-CERT VU#739844
Microsoft Windows Media Player 7.1, 8.0, 9.0, 10.0	A buffer overflow vulnerability has been reported in Windows Media Player, bitmap handling, that could let remote malicious users execute arbitrary code. Microsoft Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Media Player Arbitrary Code Execution CVE-2006-0006	Not Available	Microsoft, Security Bulletin MS06-005, February 14, 2006 Technical Cyber Security Alert TA06-045A Cyber Security Alert SA06-045A US-CERT VU#291396
Microsoft Windows Media Player XP, 2000, and Server 2003 various versions	A buffer overflow vulnerability has been reported in Windows Media Player, plugin for non-Microsoft browsers, that could let remote malicious users execute arbitrary code. Microsoft Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Media Player Arbitrary Code Execution CVE-2006-0005	Not Available	Microsoft, Security Bulletin MS06-006, February 14, 2006 Technical Cyber Security Alert TA06-045A Cyber Security Alert SA06-045A US-CERT VU#692060
Microsoft Windows Web Client XP and Server 2003 various versions	A buffer overflow vulnerability has been reported in Windows Web Client that could let local or remote malicious users to execute arbitrary code. Microsoft Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Web Client Arbitrary Code Execution CVE-2006-0013	Not Available	Microsoft, Security Bulletin MS06-008, February 14, 2006 US-CERT VU#388900
Mirabilis ICQ Lite 4.0, 4.1, 2003 a, b	A vulnerability has been reported in Mirabilis ICQ that could let remote malicious users to execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	Mirabilis ICQ Arbitrary Code Execution	Not Available	Security Focus, ID: 16655, February 15, 2006
Nullsoft Winamp 5.13	A buffer overflow vulnerability has been reported in Winamp that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	Winamp Arbitrary Code Execution CVE-2006-0708	Not Available	Security Tracker, Alert ID: 1015621, February 14, 2006
Webeveyn Whomp Real Estate Manager XP 2005	A vulnerability has been reported in Whomp Real Estate Manager XP 2005 that could let remote malicious users perform	Whomp Real Estate Manager XP 2005 SQL Injection	7	Secunia, Advisory: SA18780, February 9, 2006

	SQL injection. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	CVE-2006-0624		
Webwasher CSM Suite 5.0, CSM Appliance	A vulnerability has been reported in CSM Suite and CSM Appliance that could let remote malicious users bypass security restrictions. No workaround or patch available at time of publishing. There is no exploit code required. **Testing indicates this issues is not reproducible, and has been retired.**	WebWasher Security Bypassing CVE-2005-4514	**Retired**	Security Focus, ID: 16047, December 22, 2005 **Security Focus, ID: 16047, February 14, 2006**

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
Apple Mac OS X Server 10.4-10.4.4, 10.3-10.3.9, 10.2-10.2.8, 10.1-10.1.5, OS X 10.4-10.4.4, 10.3-10.3.9, 10.2-10.2.8, 10.1-10.1.5, 10.0-10.0.4	A Denial of Service vulnerability has been reported due to a failure to properly handle the execution of an undocumented system call. Updates available Currently we are not aware of any exploits for this vulnerability.	Apple Mac OS X Undocumented System Call Denial of Service CVE-2006-0382	Not Available	Security Focus, Bugtraq ID: 16654, February 14, 2006
Datapark Search DataparkSearch Engine 4.16-4.36	A Cross-Site Scripting vulnerability has been reported in the Search template due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Updates available There is no exploit code required.	DataparkSearch Engine Cross-Site Scripting CVE-2006-0649	2.3	Security Focus, Bugtraq ID: 16572, February 9, 2006
DocMGR DocMGR 0.54.2 & prior	A file include vulnerability has been reported in 'process.php' due to insufficient verification of the 'includeModule' and 'siteModInfo' parameters before using to include files, which could let a remote malicious user obtain sensitive information and compromise a system. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script, docmgr_0542_ incl_xpl.php, has been published.	DocMGR Remote File Include CVE-2006-0687	Not Available	Security Focus, Bugtraq ID: 16601, February 13, 2006
GnuPG GnuPG / gpg prior to 1.4.2.1	A vulnerability has been reported because 'gpgv' exits with a return code of 0 even if the detached signature file did not carry any signature (if 'gpgv" or "gpg --verify' is used), which could let a remote malicious user bypass security restrictions. Patches available There is no exploit code required; however, a Proof of Concept exploit has been published.	GnuPG Detached Signature Verification Bypass CVE-2006-0455	4.9	GnuPG Advisory, February 15, 2006
Honeyd Honeyd prior to 1.5	A vulnerability has been reported in the IP reassembly code, which could let a remote malicious user enumerate the existence of simulated Honeyd hosts. Patches available Currently we are not aware of any exploits for this vulnerability.	Honeyd IP Reassembly Remote Virtual Host Detection	Not Available	Security Focus, Bugtraq ID: 16595, February 13, 2006

Horde Project Kronolith 2.0.5, 2.0.4	HTML injection vulnerabilities have been reported due to insufficient sanitization of the calendar name and certain event data fields, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available **Debian** There is no exploit code required.	Horde Kronolith HTML Injection CVE-2005-4189	1.4	Secunia Advisory: SA17971, December 12, 2005 **Debian Security Advisory, DSA-970-1, February 14, 2006**
IBM AIX 5.3, 5.3L	A Denial of Service vulnerability has been reported due to an unspecified error in the AIX 5300-03 unix_mp and unix_64 kernels. No workaround or patch available at time of publishing. There is no exploit code required.	IBM AIX Denial of Service CVE-2006-0666	2.3	Secunia Advisory: SA18795, February 14, 2006
IBM AIX 5.3 L, 5.3, 5.2.2, 5.2 L, 5.2	A buffer overflow vulnerability has been reported in the 'ARP' command, which could let a malicious user obtain elevated privileges. Updates available Currently we are not aware of any exploits for this vulnerability.	IBM AIX ARP Buffer Overflow CVE-2006-0674	5.6	Security Focus, Bugtraq ID: 16584, February 8, 2006
Image Magick ImageMagick 6.2.4 .5	A vulnerability has been reported in the delegate code that is used by various ImageMagick utilities when handling an image filename due to an error, which could let a remote malicious user execute arbitrary commands; and a format string vulnerability has been reported when handling filenames received via command line arguments, which could let a remote malicious user execute arbitrary code. Ubuntu Debian Mandriva **Gentoo** **RedHat** There is no exploit code required.	ImageMagick Utilities Image Filename Remote Command Execution CVE-2005-4601 **CVE-2006-0082**	7 (CVE-2005-4601) **3.9** **(CVE-2006-0082)**	Secunia Advisory: SA18261, December 30, 2005 Ubuntu Security Notice, USN-246-1, January 24, 2006 Debian Security Advisory, DSA-957-1, January 26, 2006 Mandriva Security Advisory, MDKSA-2006:024, January 26, 2006 **Gentoo Linux Security Advisory, GLSA 200602-06, February 13, 2006** **RedHat Security Advisory, RHSA-2006:0178-4, February 14, 2006**
Isode M-Vault Server 11.3	A vulnerability has been reported due to an error in the LDAP server when handling certain requests, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Isode M-Vault Server LDAP CVE-2006-0710	Not Available	Secunia Advisory: SA18818 , February 14, 2006
Multiple Vendors libpng 1.0.16, 1.0.17, 1.2.6, 1.2.7	A buffer overflow vulnerability has been reported in 'png_set_strip _alpha()' when handling a PNG image file that contains alpha channels, which could let a remote malicious user cause a Denial of Service and potentially compromise a system. Update available **RedHat** Currently we are not aware of any exploits for this vulnerability.	libpng Buffer Overflow CVE-2006-0481	2.3	Secunia Advisory: SA18654, February 1, 2006 **RedHat Security Advisory, RHSA-2006:0205-4, February 13, 2006**

Multiple Vendors Linux kernel 2.6-2.6.15	An integer overflow vulnerability has been reported in 'INVALIDATE_ INODE_PAGES2' which could lead to a Denial of Service and possibly execution of arbitrary code. Fedora Mandriva **SuSE** A Proof of Concept exploit script has been published.	Linux Kernel Integer Overflow CVE-2005-3808	3.5	Fedora Update Notification, FEDORA-2005-1138, December 13, 2005 Mandriva Security Advisory, MDKSA-2006:018, January 20, 2006 **SUSE Security Announcement, SUSE-SA:2006:006, February 9, 2006**
Multiple Vendors OpenSSH 3.x, 4.x; RedHat Fedora Core3 & Core4	A vulnerability has been reported in 'scp' when performing copy operations that use filenames due to the insecure use of the 'system()' function, which could let a malicious user obtain elevated privileges. Fedora Trustix Patches available **OpenBSD** **SuSE** There is no exploit code required.	OpenSSH SCP Shell Command Execution CVE-2006-0225	4.9	Security Focus, Bugtraq ID: 16369, January 24, 2006 Fedora Security Advisory, FEDORA-2006-056, January 24, 2006 Trustix Secure Linux Security Advisory, TSLSA-2006-0004, January 27, 2006 Security Focus, Bugtraq ID: 16369, January 31, 2006 **Secunia Advisory: SA18798, February 13, 2006** **SUSE Security Announcement, SUSE-SA:2006:008, February 14, 2006**
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6-test1-test11, 2.6, 2.6.1-2.6.11; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability was reported in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability was reported in the 'setsid()' function; and a vulnerability was reported in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges. RedHat Ubuntu Conectiva SUSE Fedora Conectiva Fedora RedHat RedHat RedHat RedHat Avaya FedoraLegacy RedHat Mandriva **Trustix** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple Vulnerabilities CVE-2005-0176 CVE-2005-0177 CVE-2005-0178 CVE-2005-0204	3.3 (CVE-2005-0176) 3.3 (CVE-2005-0177) 2.3 (CVE-2005-0178) 4.9 (CVE-2005-0204)	Ubuntu Security Notice, USN-82-1, February 15, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 SUSE Security Announce-ment, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announce-ment, CLA-2005:945, March 31, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 RedHat Security Advisories, RHSA-2005:283-15 & RHSA-2005:284-11, April 28, 2005 RedHat Security Advisory,

				RHSA-2005:472-05, May 25, 2005 Avaya Security Advisory, ASA-2005-120, June 3, 2005 FedoraLegacy: FLSA:152532, June 4, 2005 RedHat Security Advisory, RHSA-2005:420-24, Updated August 9, 2005 Mandriva Linux Security Advisory, MDKSA-2005:218, November 30, 2005 **Trustix Secure Linux Security Advisory, 2006-0006, February 10, 2006**
Multiple Vendors Linux Kernel 2.6.x; RedHat Fedora Core4	A remote Denial of Service vulnerability has been reported in the 'ip_options_echo()' function due to an error when constructing an ICMP response. Updates available Fedora **Trustix** **Ubuntu** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ICMP Error Handling Remote Denial of Service CVE-2006-0454	2.3	Secunia Advisory: SA18766, February 8, 2006 **Trustix Secure Linux Security Advisory, 2006-0006, February 10, 2006** **Ubuntu Security Notice, USN-250-1, February 13, 2006**
Multiple Vendors Linux kernel 2.6-2.6.14	Multiple vulnerabilities have been reported: a Denial of Service vulnerability was reported in 'mm/mempolicy.c' when handling the policy system call; a remote Denial of Service vulnerability was reported in 'net/ipv4/fib_ frontend.c' when validating the header and payload of fib_lookup netlink messages; an off-by-one buffer overflow vulnerability was reported in 'kernel/sysctl.c,' which could let a malicious user cause a Denial of Service and potentially execute arbitrary code; and a buffer overflow vulnerability was reported in the DVB (Digital Video Broadcasting) driver subsystem, which could let a malicious user cause a Denial of Service or potentially execute arbitrary code. Updates available **SuSE** An exploit script has been published.	Linux Kernel Multiple Vulnerabilities **CVE-2005-4635** CVE-2005-3358	**2.3** (CVE-2005-4635) 3.5 (CVE-2005-3358)	Secunia Advisory: SA18216, January 4, 2006 **SUSE Security Announcement, SUSE-SA:2006:006, February 9, 2006**
Multiple Vendors Linux kernel 2.6-2.6.14 .4; SuSE Linux Professional 10.0 OSS, 10.0, Linux Personal 10.0 OSS	A vulnerability has been reported in the NFS implementation due to insufficient validation of remote user privileges before setting ACLs, which could let a remote malicious user bypass access controls. Updates available SuSE There is no exploit code required.	Linux Kernel NFS ACL Access Control Bypass CVE-2005-3623	2.3	Security Focus, Bugtraq ID: 16570, February 9, 2006 SUSE Security Announcement, SUSE-SA:2006:006, February 9, 2006
Multiple Vendors Linux kernel prior to 2.6.15	A memory disclosure vulnerability has been reported in the 'ProcFS' kernel, which could let a malicious user obtain sensitive information. Update available Fedora RedHat	Linux Kernel ProcFS Kernel Memory Disclosure CVE-2005-4605	1.6	Security Focus, Bugtraq ID: 16284, January 17, 2006 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 Ubuntu Security Notice,

	Ubuntu **SuSE** Currently we are not aware of any exploits for this vulnerability.			USN-244-1, January 18, 2006 **SUSE Security Announcement, SUSE-SA:2006:006, February 9, 2006**
Multiple Vendors Norman Ramsey Noweb 2.9 a, 2.10 c; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user overwrite critical files. Debian There is no exploit code required.	Noweb Insecure Temporary File Creation CVE-2005-3342	Not Available	Debian Security Advisory, DSA-968-1, February 13, 2006
Multiple Vendors RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; Linux kernel 2.6.9	A Denial of Service vulnerability has been reported in the 'mq_open' system call. RedHat Ubuntu **SuSE** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'mq_open' System Call Denial of Service CVE-2005-3356	1.6	Security Focus, Bugtraq ID: 16283, January 17, 2006 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 Ubuntu Security Notice, USN-244-1, January 18, 2006 **SUSE Security Announcement, SUSE-SA:2006:006, February 9, 2006**
Multiple Vendors RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; GNU Libtasn1 prior to 1.2.10, GnuTLS prior to 1.2.10	A remote Denial of Service vulnerability has been reported due to improper decoding of DER encoded data. This could possibly lead to the execution of arbitrary code. libtasn gnutls RedHat Fedora Mandriva A Proof of Concept exploit has been published.	GnuTLS libtasn1 DER Decoding Remote Denial of Service CVE-2006-0645	7	Security Tracker Alert ID: 1015612, February 11, 2006 RedHat Security Advisory, RHSA-2006:0207-01, February 10, 2006 Fedora Update Notification, FEDORA-2006-107, February 10, 2006 Mandriva Security Advisory, MDKSA-2006:039, February 13, 2006
NeoMail NeoMail 1.28	A vulnerability has been reported in 'neomail-prefs.pl' due to insufficient validation of the Session ID in the 'addfolder()' and 'deletefolder()' parameters, which could let a remote malicious user bypass certain security restrictions. Update available There is no exploit code required.	NeoMail Security Bypass CVE-2006-0711	Not Available	Secunia Advisory: SA18785, February 14, 2006
pam_mysql pam_mysql prior to 0.6.2; 0.7 - 0.7pre2	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the SQL logging facility; and a vulnerability was reported in the 'pam_get_item()' due to a double-free error in the authentication and authentication token alteration code when handling a pointer, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. Updates available Currently we are not aware of any exploits for these vulnerabilities.	PAM-MySQL SQL Logging & Double-Free CVE-2006-0056	7	Secunia Advisory: SA18598, February 9, 2006
PowerD PowerD 2.0.2	A format string vulnerability has been reported in 'powerd.c' when logging input received via the 'WHATIDO' command, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of	PowerD Remote Format String CVE-2006-0681	Not Available	Secunia Advisory: SA18841, February 13, 2006

	publishing. An exploit script, gexp-powerd.c, has been published.			
PyBlosxom PyBlosxom 1.3.1, 1.3	An information disclosure vulnerability has been reported in 'PATH_INFO' when it contains multiple '/' at the beginning, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	PyBlosxom Information Disclosure CVE-2006-0707	Not Available	Secunia Advisory: SA18858, February 14, 2006
Royal Institute of Technology Heimdal prior to 0.6.6 & 0.7.2	A vulnerability has been reported in the 'rshd' server when storing forwarded credentials due to an unspecified error, which could let a malicious user obtain elevated privileges. Update to version 0.7.2 or 0.6.6. **Ubuntu** Currently we are not aware of any exploits for this vulnerability.	Heimdal RSHD Server Elevated Privileges CVE-2006-0582	1.6	Security Tracker Alert ID: 1015591, February 7, 2006 **Ubuntu Security Notice, USN-247-1, February 09, 2006**
scponly scponly 4.1 & prior	Several vulnerabilities have been reported: a vulnerability was reported in 'scponlyc' due to a design error, which could let a malicious user execute arbitrary code with root privileges; and a vulnerability was reported due to an error in the validation of user-supplied command line, which could let a malicious user bypass security restrictions. Upgrades available Gentoo **Debian** There is no exploit code required.	scponly Privilege Escalation & Security Bypass CVE-2005-4532 CVE-2005-4533	7 (CVE-2005-4532) 7 (CVE-2005-4533)	Secunia Advisory: SA18223, December 23, 2005 Gentoo Linux Security Advisory, GLSA 200512-17, December 29, 2005 **Debian Security Advisory, DSA-969-1, February 13, 2006**
Siteframe Siteframe Beaumont 5.0.1	A Cross-Site Scripting vulnerability has been reported in 'search.php' due to insufficient sanitization of the 'q' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Siteframe Beaumont Cross-Site Scripting CVE-2006-0675	2.3	Security Focus, Bugtraq ID: 16596, February 13, 2006
Sun Microsystems, Inc. Solaris 10.0 _x86, 10.0	A vulnerability has been reported in 'in.rexecd' due to an unspecified error, which could let a malicious user execute arbitrary commands with elevated privileges on Kerberos systems. Updates available Currently we are not aware of any exploits for this vulnerability.	Sun Solaris 'in.rexecd' Elevated Privileges	Not Available	Sun(sm) Alert Notification Sun Alert ID: 102186, February 14, 2006
SuSE Novell Linux Desktop 1.0, Linux Professional 10.0, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1	A buffer overflow vulnerability has been reported in the 'nfs-server,' which could let a remote malicious user execute arbitrary code. SUSE **Debian** Currently we are not aware of any exploits for this vulnerability.	SUSE NFS-SERVER Remote Buffer Overflow CVE-2006-0043	4.9	SuSE Security Announcement, SUSE-SA:2006:005, January 25, 2006 **Debian Security Advisory, DSA-975-1, February 15, 2006**

SuSE Novell Linux Desktop 9.0, Linux Professional 10.0 OSS, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, 9.0 x86_64, 9.0, Linux Personal 10.0 OSS, .3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, 9.0 x86_64, 9.0	A vulnerability has been reported because LD sometimes leaves empty RPATH components in certain binaries, which could let a malicious execute arbitrary code. SuSE There is no exploit code required.	SUSE LD Insecure RPATH / RUNPATH Arbitrary Code Execution CVE-2006-0646	3.9	SuSE Security Announcement, SUSE-SA:2006:007, February 10, 2006
Virtual Hosting Control System Virtual Hosting Control System 2.4.7 .1, 2.4.6 .2, 2.2	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the login page due to insufficient sanitization of the username field before storing in the admin log, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported in the 'gui/admin/change _password.php' script due to insufficient validation of the user's password before allowing the password to be changed, which could let a remote malicious user bypass authentication; a vulnerability was reported in 'gui/include/login.php' due to insufficient termination of the 'check_login()' function when the user session validation fails, which could let a remote malicious bypass authentication; and a vulnerability was reported in the 'gui/admin/add_user.php' script due to insufficient validation of user's rights before allowing admin users to be added, which could let a remote malicious user add new admin users to the system. Patches available (this does not fix the 'gui/admin/chang e_password.php' script vulnerabilities) There is no exploit code required; however, Proof of Concept exploits and an exploit script, rs_vhcs_simple_poc.html, have been published.	Virtual Hosting Control System Multiple Input Validation & Access Validation CVE-2006-0683 CVE-2006-0684 CVE-2006-0685 CVE-2006-0686	Not Available	Security Focus, Bugtraq ID: 16600, February 13, 2006

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Description	Common Name	CVSS	Resources
2200net Calendar 2200net Calendar 1.2	SQL injection vulnerabilities have been reported in 'main.php' due to insufficient sanitization of the 'username' and 'password' fields during login and the 'fm_data[id]' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	2200net Calendar System SQL Injection CVE-2006-0610	7	Secunia Advisory: SA18781, February 9, 2006
Ansilove Ansilove prior to 1.03	Several vulnerabilities have been reported: a vulnerability was reported in the loaders script, (load_*.php) due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information; and a vulnerability was reported due to insufficient sanitization of the filenames of uploaded files, which could let a remote malicious user execute arbitrary PHP code. Updates available There is no exploit code required.	Ansilove File Disclosure & File Upload CVE-2006-0694 CVE-2006-0695	2.3 (CVE-2006-0694) 7 (CVE-2006-0695)	Security Focus, Bugtraq ID: 16603, February 13, 2005
Chain Reaction Edition CRE Loaded 6.15	A vulnerability has been reported in the '/admin/htmlarea/popups/ file/files.php' script due to insufficient authentication, which could let a remote malicious user upload/create/delete arbitrary files. **Patch available** There is no exploit code required.	CRE Loaded Files.PHP Access Validation CVE-2006-0478	7	Secunia Advisory: SA18648, January 30, 2006 **Security Focus, Bugtraq ID: 16415, February 7, 2006**

Cisco Systems Traffic Anomaly Detector Module 5.0(3), 5.0(1), Traffic Anomaly Detector 5.0(3), 5.0(1), Cisco Guard 5.0(3), 5.0(1), Cisco Anomaly Guard Module 5.0(3), 5.0(1)	A vulnerability has been reported when the devices have been configured to authenticate users against an external TACACS+ server but an external TACACS+ server is not specified in the configuration using the tacacs-server host command, which could let a remote malicious user obtain unauthorized access to devices or obtain elevated privileges. Update information available There is no exploit code required.	Cisco Multiple Products TACACS+ Authentication Bypass	Not Available	Cisco Security Advisory, cisco-SA-20060215, February 15, 2006
Clever Copy Clever Copy 2.0 a, 2.0	An HTTP injection vulnerability has been reported due to insufficient sanitization of the 'Referer' and 'X-Forwarded-For' HTTP headers before using, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Clever Copy HTML Injection CVE-2006-0627	2.3	Secunia Advisory: SA18790, February 10, 2006
contentServ contentServ 3.1	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. **The vendor has released a hotfix to address this issue. Contact the vendor for further information.** There is no exploit code required.	ContentServ SQL Injection CVE-2005-4390	7	Security Focus, Bugtraq ID: 15956, December 19, 2005 **Security Focus, Bugtraq ID: 15956, February 8, 2006**
CPAINT CPAINT prior to 2.0.3	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'cpaint_response_type' parameter in a script using the affected library, which could let a remote malicious user execute arbitrary HTML and script code. Updates available There is no exploit code required; however, a Proof of Concept exploit has been published.	CPAINT Cross-Site Scripting CVE-2006-0650	2.3	GulfTech Security Research Team Advisory, February 9, 2006
CPG-Nuke Dragonfly CMS 9.0.6 .1	A file include vulnerability has been reported in the 'install.php' script due to insufficient validation of the 'newlang' parameter and in the 'installlang' cookie parameter, which could let a remote malicious user execute arbitrary PHP code. Patches available There is no exploit code required; however, a Proof of Concept exploit scripts, cpg_dragonfly_exploit.php and dragonfly9.0.6.1_incl_xpl.html, have been published.	CPG Dragonfly File Include CVE-2006-0644	7	Security Tracker Alert ID: 1015601, February 8, 2006
David Barrett QwikiWiki 1.5	A Cross-Site Scripting vulnerability has been reported in 'search.php' due to insufficient sanitization of the 'query' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	QwikiWiki Cross-Site Scripting CVE-2006-0699	Not Available	Security Focus, Bugtraq ID: 16638, February 14, 2006
DeltaScripts PHP Classifieds 6.20	An SQL injection vulnerability has been reported in 'member_login.php' due to insufficient sanitization of the 'username' and 'password' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. DeltaScripts Workaround There is no exploit code required; however, a Proof of Concept exploit has been published.	DeltaScripts PHP Classifieds SQL Injection CVE-2006-0719	Not Available	Security Focus, Bugtraq ID: 16642, February 14, 2005
Dotproject Dotproject 2.0.1, 2.0	Several vulnerabilities have been reported: a file include vulnerability was reported in 'baseDir' parameter in '/includes/db_adodb.php,' '/includes/db_connect.php,' '/includes/session.php,' '/modules/admin/vw_usr_roles.php,' '/modules/public/calendar.php,' and '/modules/public/date_format.php' due to insufficient verification before using to include files, which could let a remote malicious user execute arbitrary code; a file include vulnerability was reported in the 'dPconfig[root_dir]' parameter in	Dotproject File Include & Information Disclosure	Not Available	Secunia Advisory: SA18879, February 15, 2006

	'/modules/projects/gantt.php,' '/modules/projects/gantt2.php,' '/modules/projects/vw_files.php,' and '/modules/tasks/gantt.php' due to insufficient verification before using to include files, which could let a remote malicious user execute arbitrary code; a vulnerability was reported when accessing '/docs/phpinfo.php' and '/docs/check.php' which could lead to the disclosure of system configuration information; and a vulnerability was reported when PHP 'display_errors' is enabled and '/db/' directory files are accessed with certain parameters, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.			
e107.org e107 website system 0.x	HTML injection vulnerabilities have been reported due to insufficient sanitization of certain BBcode before using, which could let a remote malicious user execute arbitrary HTML and script code. Updates available There is no exploit code required.	e107 BBCode HTML Injection CVE-2006-0682	Not Available	Secunia Advisory: SA18816, February 13, 2006
FarsiNews FarsiNews 2.5, 2.1 Beta2, 2.1	Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information; and a file include vulnerability was reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user include arbitrary files. The vendor has released an update to address this issue. Please contact the vendor for further information. There is no exploit code required; however, a Proof of Concept exploit has been published.	FarsiNews Directory Traversal & File Include CVE-2006-0660	4.7	Security Focus, Bugtraq ID: 16580, February 13, 2006
Fortinet FortiOS 3.0 beta, 2.8 MR10	Several vulnerabilities have been reported: a vulnerability was reported because the URL blocking functionality can be bypassed, which could let a remote malicious user bypass antivirus protection; and a vulnerability was reported because the virus scanning functionality can be bypassed when FTP files are sent under certain conditions. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploit scripts, http_req.pl and Fortinet-url.txt, have been published.	FortiGate URL Filter & Virus Scanning Bypass CVE-2005-3057 CVE-2005-3058	Not Available	Secunia Advisory: SA18844, February 13, 2006
Francisco Burzi PHP-Nuke 7.8 & prior	A Cross-Site Scripting vulnerability has been reported in 'header.php' due to insufficient sanitization of the 'pagetitle' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPNuke Cross-Site Scripting CVE-2006-0676	2.3	Security Focus, Bugtraq ID: 16608, February 13, 2006
Hinton Design phphd 1.0	Multiple vulnerabilities have been reported: an SQL injection vulnerability was reported in 'check.php' due to insufficient sanitization of the 'username' parameter during login and other unspecified parameters, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in 'check.php' due to an error in the authentication process, which could let a remote malicious user bypass the authentication process; and a Cross-Site Scripting vulnerability was reported in 'add.php' due to insufficient sanitization of unspecified parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Hinton Design PHPHD Multiple Input Validation & Authentication Bypass CVE-2006-0607 CVE-2006-0608 CVE-2006-0609	7 (CVE-2006-0607) 7 (CVE-2006-0608) 2.3 (CVE-2006-0609)	Secunia Advisory: SA18793, February 10, 2006

Hinton Design phpht topsites 1.3	Multiple vulnerabilities have been reported: an SQL injection vulnerability was reported in the 'username' parameter due to insufficient sanitization before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in 'check.php' due to an error in the authentication process, which could let a remote malicious user obtain unauthorized access; a Cross-Site Scripting vulnerability was reported in 'link_edited.php' and 'link_added.php' due to insufficient sanitization before using, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	phpht Topsites Input Validation CVE-2006-0653 CVE-2006-0654 CVE-2006-0655	7 (CVE-2006-0653) 7 (CVE-2006-0654) 2.3 (CVE-2006-0655)	Secunia Advisory: SA18782, February 9, 2006
Hinton Design phpstatus 1.0	Multiple vulnerabilities have been reported: an SQL injection vulnerability was reported in 'check.php' due to insufficient sanitization of the 'username' parameter during login before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in 'check.php' due to an error in the authentication process, which could let a remote malicious user bypass the authentication process; and a Cross-Site Scripting vulnerability was reported in the administration section due to insufficient sanitization of unspecified parameters and scripts before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Hinton Design PHPStatus Multiple Input Validation CVE-2006-0570 CVE-2006-0571 CVE-2006-0572	7 (CVE-2006-0570) 2.3 (CVE-2006-0571) 7 (CVE-2006-0572)	Secunia Advisory: SA18791, February 10, 2006
Hitachi, Ltd. Hitachi Business Logic - Container 03-00-/B, 03-00, 02-03	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of unspecified input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported due to insufficient sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrade information There is no exploit code required.	Hitachi Business Logic Cross-Site Scripting & SQL Injection CVE-2005-4716	Not Available	HS06-002, Hitachi Security Advisory, February 13, 2006
HiveMail HiveMail 1.2.2, 1.3 RC1, 1.3 Beta 1, 1.3	Several vulnerabilities have been reported: a vulnerability was reported in 'addressbook.update.php' due to insufficient sanitization of the 'contactgroupid' parameter, in 'addressbook.add.php' due to insufficient sanitization of the 'messageid' parameter, in 'folders.update.php' due to insufficient sanitization of the 'folderid' parameter, and in the 'calendar.event.php,' index.php,' 'pop.download.php,' 'read.bounce.php,' 'rules.block.php' and 'language.php' scripts due to insufficient sanitization, which could let a remote malicious user execute arbitrary PHP code; and a Cross-Site Scripting and SQL injection vulnerability was reported due to insufficient sanitization of the '$_SERVER['PHP_SELF']' references, which could let a remote malicious user execute arbitrary HTML, script code, and SQL code. No workaround or patch available at time of publishing. Proof of Concept exploits have been published.	HiveMail Multiple Vulnerabilities	Not Available	GulfTech Security Research Team Advisory, February 10, 2006
IBM Domino Web Access 6.5.1-6.5.4, 6.0.1-6.0.5, 7.0, 6.5, 6.0	Multiple vulnerabilities have been reported: a vulnerability was reported because attached files can be opened in the context of the site if the user clicks on it, which could lead to the execution of arbitrary JavaScript code; a vulnerability was reported due to insufficient sanitization of the email subject before displaying to the user as the browser title, which could lead to the execution of arbitrary JavaScript; a vulnerability was reported because it is possible to bypass certain security checks related to 'javascript:' URLs, which could lead to the execution of arbitrary JavaScript code; a vulnerability was reported due to insufficient sanitization of the attachment filename before displaying to the user, which could lead to the execution of arbitrary JavaScript; and a remote Denial of Service vulnerability was reported in the LDAP service when processing bind requests due to a NULL pointer dereference.	IBM Lotus Domino iNotes Multiple HTML & Script Injection CVE-2005-2712	Not Available	Secunia Advisory: SA16340, February 10, 2006

	Patch information There is no exploit code required: however Proof of Concept exploits have been published.			
IBM Tivoli Directory Server 6.0 .0	A Denial of Service vulnerability has been reported in the LDAP server due to an error when handling certain requests. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	IBM Tivoli Directory Server LDAP Denial of Service CVE-2006-0717	Not Available	Secunia Advisory: SA18779, February 13, 2006
IBM Lotus Notes 6.x, 7.x	Multiple vulnerabilities have been reported: a vulnerability was reported in 'kvarcve.dll' when constructing the full pathname of a compressed file to check for its existence before extracting it from a ZIP archive, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in 'uudrdr.dll' when handling 'UUE' files that contain an encoded file with an overly long filename, which could let a remote malicious user execute arbitrary code; a Directory Traversal vulnerability was reported in 'kvarcve.dll' when generating the preview of a compressed file from ZIP, UUE, and TAR archives, which could let a remote malicious user delete arbitrary files; a vulnerability was reported in the 'TAR' reader when extracting files from a TAR archive that contain a long filename, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in the HTML speed reader due to a boundary error, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported in the HTML speed reader when checking if a link references a local file due to a boundary error, which could let a remote malicious user execute arbitrary code. These issues have been addressed in Lotus Notes versions 6.5.5 and 7.0.1. Please contact the vendor to obtain fixes. Currently we are not aware of any exploits for these vulnerabilities.	IBM Lotus Notes Multiple Vulnerabilities CVE-2005-2618 CVE-2005-2619	Not Available	Secunia Advisory: SA16280, February 10, 2006 US-CERT VU#884076
ImageVue ImageVue 0.16.1	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'dir.php' and 'readfolder.php' scripts because a remote malicious user can obtain sensitive information; a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient sanitization of the 'bgcol' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'admin.upload.php' due to insufficient sanitization of the file extension, which could let a remote malicious user upload arbitrary files. No workaround or patch available at time of publishing. Proof of Concept exploits have been published.	ImageVue Multiple Vulnerabilities CVE-2006-0700 CVE-2006-0701 CVE-2006-0702 CVE-2006-0703	Not Available	Secunia Advisory: SA18802, February 14, 2006
Invision Power Services Invision Board 2.0.1	A remote Denial of Service vulnerability has been reported in user registration. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script, IPB_sedXPL.pl, has been published.	Invision Power Board User Registration Remote Denial of Service	Not Available	Security Focus, Bugtraq ID: 16616, February 14, 2006
Lawrence Osiris DB_eSession 1.0.2	An SQL injection vulnerability was reported due to insufficient sanitization of the 'deleteSession()' function before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Lawrence Osiris DB_eSession SQL Injection	Not Available	Security Focus, Bugtraq ID: 16598, February 13, 2006
LinPHA LinPHA 0.9.0-0.9.4, 1.0	A vulnerability has been reported in 'docs/index.php' due to insufficient verification of the 'lang' parameter before used to include files, which could let a remote malicious user include arbitrary files and execute arbitrary PHP code. No workaround or patch available at time of publishing.	LinPHA File Inclusion & PHP Code Injection CVE-2006-0713	Not Available	Security Focus, Bugtraq ID: 16592, February 13, 2006

	A Proof of Concept exploit script, linpha_10_local.txt, has been published.			
Mantis Mantis 1.0.0 RC4, RC3, 1.0 .0rc2, rc1, a1-a3, 0.10-0.19.4, 0.9.1, 0.9	A Cross-Site Scripting vulnerability has been reported in 'config_defaults _inc.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. Updates available There is no exploit code required.	Mantis Cross-Site Scripting CVE-2006-0664 CVE-2006-0665	2.3 (CVE-2006-0664) 4.9 (CVE-2006-0665)	Security Focus, Bugtraq ID: 16561, February 9, 2006
Mantis Mantis 1.00rc4 & prior	Multiple input validation vulnerabilities have been reported including Cross-Site Scripting in 'view_all_set.php,' 'manage_user_page.php,' and 'proj_doc_delete.php' and SQL injection in 'manage_user_page.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML, script code, and SQL code. Updates available There is no exploit code required; however, Proof of Concept exploits have been published.	Mantis Multiple Input Validation	Not Available	BuHa Security-Advisory #7, February 14, 2006
Metamail Metamail 2.7	A buffer overflow vulnerability has been reported when handling boundary headers within email messages, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Metamail Remote Buffer Overflow CVE-2006-0709	Not Available	Security Focus, Bugtraq ID: 16611, February 13, 2006
Multiple Vendors Flyspray 0.9.7; Enterprise Groupware Systems EGS 1.0 rc4	A file include vulnerability has been reported in the ADODBPath due to insufficient sanitization of user-supplied input, which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploit scripts, egs_10rc4_php5_ incl_xpl.php and flyspray_097_php5 _incl_xpl.php, have been published.	Flyspray ADODBPath Remote File Include CVE-2006-0714	Not Available	Security Focus, Bugtraq ID: 16618, February 14, 2006
Multiple Vendors SSH Communications SSH Tectia Server 4.4.0 (A & T), 4.3.6 (A & T) & prior, SSH Secure Shell Server 3.2.9 & prior; Attachmate WRQ Reflection for Secure IT UNIX Server version 6.0, Windows Server version 6.0	A vulnerability has been reported in the SFTP component during logging of accessed file names due to an unspecified error, which could let a remote malicious user execute arbitrary code. SSH Communications Reflection for Secure IT Currently we are not aware of any exploits for this vulnerability.	SSH Tectia Server SFTP Logging Arbitrary Code Execution CVE-2006-0705	Not Available	Security Tracker Alert ID: 1015619, February 13, 2006 US-CERT VU#419241
Multiple Vendors Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha; adzapper 20060115, 20050316, 20030726	A remote Denial of Service vulnerability has been report in the 'squid_redirect' script when handling URLs that contain a large number of forward slashes. Adzapper Debian There is no exploit code required.	Adzapper Remote Denial of Service CVE-2006-0046	3.3	Security Focus, Bugtraq ID: 16558, February 9, 2006 Debian Security Advisory, DSA-966-1, February 9, 2006

Multiple Vendors Elog Web Logbook prior to 2.5.7 r1558-4; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	Multiple vulnerabilities have been reported: several buffer overflow vulnerabilities were reported in 'elogd.c' due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code; a buffer overflow vulnerability was reported in 'elogd.c' when writing to the log file, which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code; a vulnerability was reported in 'elog.c' and 'elogd.c' because different responses are generated depending on whether or a username is valid, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability was reported in 'elogd.c' when handling the 'fail' parameter. Debian Exploitation of some of these issues does not require exploit code.	ELOG Web Logbook Multiple Remote CVE-2006-0597 CVE-2006-0598 CVE-2006-0599 CVE-2006-0600	7 (CVE-2006-0597) 7 (CVE-2006-0598) 2.3 (CVE-2006-0599) 2.3 (CVE-2006-0600)	Debian Security Advisory, DSA-967-1, February 10, 2006
Multiple Vendors PostNuke Development Team PostNuke 0.761; moodle 1.5.3; Mantis 1.0.0RC4, 0.19.4; Cacti 0.8.6 g; ADOdb 4.68, 4.66; AgileBill 1.4.92 & prior	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in the 'server.php' test script, which could let a remote malicious user execute arbitrary SQL code and PHP script code; and a vulnerability was reported in the 'tests/tmssql.php' text script, which could let a remote malicious user call an arbitrary PHP function. Adodb Cacti Moodle PostNuke AgileBill **Mantis** There is no exploit code required; however, a Proof of Concept exploit has been published.	ADOdb Insecure Test Scripts CVE-2006-0146 CVE-2006-0147	7 (CVE-2006-0146) 7 (CVE-2006-1047)	Secunia Advisory: SA17418, January 9, 200 Security Focus, Bugtraq ID: 16187, February 7, 2006 **Security Focus, Bugtraq ID: 16187, February 9, 2006**
Multiple Vendors U.S.Robotics USR80540; D-Link DI-784 0, DI-624 0, DI-524 3.20, DI-524 0	A remote Denial of Service vulnerability has been reported when attempting to reassemble certain IP packets. No workaround or patch available at time of publishing. There is no exploit code required; however, an exploit script, dlink_udp_dos.c, has been published.	Multiple D-Link Products Remote Denial of Service CVE-2005-4723	Not Available	Security Focus, Bugtraq ID: 16621, February 14, 2006
Nicecoder indexu 5.0.1, 5.0	A file include vulnerability has been reported in 'Application.PHP' due to insufficient verification of the 'base_path' parameter, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Indexu File Include CVE-2006-0688	7	ECHO_ADV_ 26$2006, February 9, 2006
Nokia Nokia N70	Several vulnerabilities have been reported: a vulnerability was reported in the Bluetooth stack when handling certain requests, which could lead to a remote Denial of Service or a 'System Error' message displayed; and a remote Denial of Service vulnerability was reported in the Bluetooth stack when handling short malformed L2CAP packets. No workaround or patch available at time of publishing. Exploit scripts, loop.sh and replay_l2cap_packet _nokiaN70.c, have been	Nokia Cell Phones Bluetooth Denials of Service	Not Available	Secunia Advisory: SA18724, February 14, 2006
OTRS OTRS (Open Ticket Request System) 2.0.0-2.0.3, 1.3.2, 1.0 .0	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in the 'login' function due to insufficient sanitization of the 'login' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; an SQL injection vulnerability was reported in the 'AgentTicketPlain' function due to insufficient sanitization of the 'TicketID' and 'ArticleID' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of HTML email attachments before displaying, which could let a remote malicious user execute arbitrary HTML	OTRS SQL Injection & Cross-Site Scripting CVE-2005-3893 CVE-2005-3894 CVE-2005-3895	7 (CVE-2005-3893) 2.3 (CVE-2005-3894) 2.3 (CVE-2005-3895)	OTRS Security Advisory, OSA-2005-01, November 22, 2005 SUSE Security Summary Report, SUSE-SR:2005:030, December 16, 2005 **Debian Security Advisory, DSA-973-1, February**

	and script code; and a Cross-Site Scripting vulnerability was reported in 'index.pl' due to insufficient sanitization of the 'QueueID' and 'Action' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available SUSE **Debian** There is no exploit code required; however, Proof of Concept exploits have been published.			**15, 2006**
Papoo Papoo 2.1.2	Cross-Site Scripting vulnerabilities have been reported in new account registration due to insufficient sanitization of the username field, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Papoo Multiple Cross-Site Scripting CVE-2006-0569	2.3	Security Focus, Bugtraq ID: 16573, February 9, 2006
PHP iCalendar PHP iCalendar 2.0.1, 2.1, 2.0	A file include vulnerability has been reported in 'functions/template.php' due to insufficient verification of the 'file' parameter and in 'serach.php' due to insufficient verification of the 'getdate' parameter, which could let a remote malicious user execute arbitrary PHP code. Updates available There is no exploit code required.	PHP ICalendar Remote File Include CVE-2006-0648	2.3	Secunia Advisory: SA18778, February 10, 2006
PHP4Scripte.de Gastebuch 1.3.2	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'URL' field, which could let a remote malicious user execute arbitrary HTML and script code. Update available There is no exploit code required; however, a Proof of Concept exploit has been published.	Gastebuch Cross-Site Scripting CVE-2006-0706	Not Available	Security Focus, Bugtraq ID: 16615, February 14, 2006
PHP-MySQL Timesheet PHP-MySQL Timesheet 2.0, 1.0	SQL injection vulnerabilities have been reported due to insufficient sanitization of the 'yr,' 'month,' 'day,' and 'job' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	PHP/MYSQL Timesheet Multiple SQL Injection CVE-2006-0692	7	Secunia Advisory: SA18822, February 13, 2006
Plume CMS Plume CMS 1.0.2	A vulnerability has been reported in 'prepend.php' due to insufficient verification of the '_PX_config[manager_path]' parameter before using to include files, which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required.	Plume CMS File Include CVE-2006-0725	Not Available	Security Focus, Bugtraq ID: 16662, February 15, 2006
PostgreSQL PostgreSQL 8.1.2, 8.1.1, 8.1	Several vulnerabilities have been reported: a vulnerability was reported in the 'SET ROLE" command when previous role settings are restored after an error, which could let a malicious user obtain superuser privileges; and a Denial of Service vulnerability was reported due to an error in the 'SET SESSION AUTHORIZATION' command if compiled with 'Asserts' enabled. Updates available There is no exploit code required.	PostgreSQL Privilege Escalation & Denial of Service CVE-2006-0553 CVE-2006-0678	Not Available	Secunia Advisory: SA18890, February 15, 2006
PwsPHP PwsPHP 1.2.3	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit and an exploit script, PwsPHP_SQL_Inj.php, have been published.	PwsPHP SQL Injection CVE-2006-0668	7	Security Focus, Bugtraq ID: 16567, February 9, 2006
Reamday Enterprises Magic Calendar Lite	An SQL injection vulnerability has been reported in 'cms/index.php' due to insufficient sanitization of the 'total_login' and 'total_password' parameters before using	Magic Calendar Lite SQL	7	Secunia Advisory: SA18855, February 14, 2006

1.02	in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Injection CVE-2006-0673		
Reamday Enterprises Magic News Lite 1.2.3	Several vulnerabilities have been reported: a file include vulnerability was reported in 'preview.php' due to insufficient verification on of the 'php_script_path' parameter before using to include files, which could let a remote malicious user include arbitrary files; and a vulnerability was reported in 'profile.php' due to insufficient initialization of the '$passwd,' '$admin_password,' '$new_passwd,' and '$confirm_passwd' variables, which could let a remote malicious user change the administrator's password. No workaround or patch available at time of publishing. There is no exploit code required.	Reamday Enterprises Magic News Lite File Include & Profile Update CVE-2006-0724 CVE-2006-0723	1.9 (CVE-2006-0724) 1.9 (CVE-2006-0723)	Secunia Advisory: SA18878, February 15, 2006
Reamday Enterprises Magic News Lite 1.2.3, Magic Downloads 1.1.3	Multiple vulnerabilities have been reported regarding the overwriting of application variables due to insufficient initialization of various application variables, which could let a remote malicious user obtain administrative access. No workaround or patch available at time of publishing. There is no exploit code required.	Multiple Reamday Enterprises Products Variable Overwrite CVE-2006-0724 CVE-2006-0723 CVE-2006-0722	1.9 (CVE-2006-0724) 1.9 (CVE-2006-0723) 1.9 (CVE-2006-0722)	Security Focus, Bugtraq ID: 16665, February 15, 2006
Research In Motion Blackberry Enterprise Server for Novell Groupwise 4.0, SP1-SP3, Blackberry Enterprise Server for Exchange 4.0, SP1-SP3, 3.6.1, 3.6 SP4 Hot Fix 2, 3.6 SP 1a, 3.6, Blackberry Enterprise Server for Domino 4.0, SP1-SP3, 2.2 SP4 Hot Fix 2, 2.2 SP4, SP3a, SP2a, SP2, 2.2	A buffer overflow vulnerability has been reported in the BlackBerry Attachment Service when processing a malformed Word document, which could let a remote malicious user execute arbitrary code. Upgrade information available Currently we are not aware of any exploits for this vulnerability.	BlackBerry Enterprise Server Malformed Word Attachment Buffer Overflow	Not Available	Black Knowledge Base Article, KB-04791, February 9, 2006
Roberto Butti CALimba 0.99.2 beta & prior	SQL injection vulnerabilities have been reported in 'rb/cls/rb_auth.php' due to insufficient sanitization of the 'login' and 'password' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	CALimba SQL Injection CVE-2006-0693	7	Secunia Advisory: SA18856, February 14, 2006
RunCMS RunCMS 1.3a3	An SQL injection vulnerability has been reported in '/modules/messages /pmlite.php' due to insufficient sanitization of the 'to_userid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	RunCMS SQL Injection CVE-2006-0721	7	Secunia Advisory: SA18831, February 14, 2006
RunCMS RunCMS 1.2 & prior	Several vulnerabilities have been reported: a vulnerability was reported in the 'FCKEDITOR' connector because it is possible to upload arbitrary files, which could let a remote malicious user execute arbitrary PHP code; and a vulnerability was reported in 'class.forumposts.php' due to insufficient verification of the 'bbPath[path]' parameter and in 'forumpoll renderer.php' due to insufficient verification of the 'xoopsConfig [language] parameter, which could let a remote malicious user include arbitrary files. Updates available	RunCMS Remote Code Execution CVE-2006-0658 CVE-2006-0659	2.3 (CVE-2006-0658) 7 (CVE-2006-0659)	Secunia Advisory: SA18800, February 10, 2006

	Proof of Concept exploit scripts, fckeditor_22_xpl.php and runcms_13a_xpl.php have been published.			
Scheduling Management Time Tracking Software 3.0	Multiple vulnerabilities have been reported: a vulnerability was reported in 'edituser.php' due to insufficient credential validation, which could let a remote malicious user modify data; SQL injection vulnerabilities were reported in several unspecified parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in the Registration Form due to insufficient sanitization of the UserName field before saving, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Time Tracking Software Multiple Input Validation CVE-2006-0689 CVE-2006-0690 CVE-2006-0691	2.3 (CVE-2006-0689) 7 (CVE-2006-0690) 2.3 (CVE-2006-0691)	Security Focus, Bugtraq ID: 16630, February 14, 2006
scriptme SmE GB Host 1.21	An SQL injection vulnerability has been reported in 'login.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Scriptme SmE GB Host SQL Injection	Not Available	Security Focus, Bugtraq ID: 16609, February 13, 2006
scriptme SmE GB Host 1.21, SmE Blog Host 0	A Cross-Site Scripting vulnerability has been reported in the BBcode URL tag due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Scriptme Applications Cross-Site Scripting CVE-2006-0661	2.3	Security Focus, Bugtraq ID: 16585, February 13, 2006
Softcomplex PHP Event Calendar 1.5	An HTML injection vulnerability has been reported due to insufficient sanitization of the 'username' and 'password' fields when updating user information before storing, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	PHP Event Calendar HTML Injection CVE-2006-0657	1.4	Security Focus, Bugtraq ID: 16588, February 13, 2006
Solucija sNews 1.3	Multiple input validation vulnerabilities have been reported due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML, script code, and SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	sNews Multiple Input Validation CVE-2006-0715 CVE-2006-0716	Not Available	Security Focus, Bugtraq ID: 16647, February 14, 2006
SPIP SPIP 1.8.2g & prior	Several vulnerabilities have been reported: a vulnerability was reported in 'spip_rss.php' due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary PHP code; and an SQL injection vulnerability was reported in 'spip_acces_doc.php3' due to insufficient validation of the 'file' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits and an exploit script, spip_182g_shell_inj_xpl.php, have been published.	SPIP Arbitrary Code Execution CVE-2006-0625 CVE-2006-0626	4.7 (CVE-2006-0625) 7 (CVE-2006-0626)	Security Tracker Alert ID: 1015602, February 9, 2006
Sun Microsystems, Inc. Java Web Start 1.x, Java JDK 1.5.x, Java JRE 1.5.x / 5.x	A vulnerability has been reported due to an unspecified error, which could let an untrusted application obtain elevated privileges. Updates available Currently we are not aware of any exploits for this vulnerability.	Java Web Start Sandbox Security Bypass CVE-2006-0613	**2.6**	Sun(sm) Alert Notification Sun Alert ID: 102170, February 7, 2006 **US-CERT VU#652636**
Sun Microsystems, Inc. Sun JDK & JRE 5.0 Update 5 & prior, SDK & JRE 1.4.2_09 & prior, SDK & JRE	Seven vulnerabilities have been reported in Sun Java JRE (Java Runtime Environment) due to various unspecified errors in the 'reflection' APIs, which could let a remote malicious user compromise a user's system. Update information	Sun Java JRE 'reflection' APIs Sandbox Security Bypass CVE-2006-0614	**4.7** (CVE-2006-0614) **2.6** (CVE-2006-0615)	Sun(sm) Alert Notification Sun Alert ID: 102171, February 7, 2006 **Gentoo Linux Security Advisory,**

1.3.1_16 & prior	**Gentoo** Currently we are not aware of any exploits for these vulnerabilities.	CVE-2006-0615 CVE-2006-0616 CVE-2006-0617	**2.6** (CVE-2006-0616) **2.6** (CVE-2006-0617)	**GLSA 200602-07, February 15, 2006** **US-CERT VU#759996**
Sun Microsystems, Inc. Sun ONE Directory Server 5.2 patch 3 & patch 4, 5.2, 5.2 2005Q1, Java System Directory Server 5.2 2004Q2, 5.2 2003Q4, Sun Java System Directory Server 5.2	A remote Denial of Service vulnerability has been reported due to a failure to handle malformed network traffic. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Sun ONE Directory Server Remote Denial of Service	Not Available	Security Focus, Bugtraq ID: 16550, February 10, 2006
supersmash brothers IPB Army System 2.1 & prior	An SQL injection vulnerability has been reported in 'army.php' due to insufficient sanitization of the 'userstat' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, exploit scripts, ipb_army_ 2.1_sql_expl.php and ArmySystem v2.1.txt, have been published.	IPB Army System SQL Injection	Not Available	Security Focus, Bugtraq ID: 16606, February 13, 2006
Valve Software CSTRIKE Dedicated Server 1.6 Windows, CSTRIKE Dedicated Server 1.6 Linux	A remote Denial of Service vulnerability has been reported in the CSTRIKE dedicated server. No workaround or patch available at time of publishing. An exploit scripts, csdos.pl and halfLifeDoS.txt , have been published.	Valve Software Half-Life CSTRIKE Server Remote Denial of Service CVE-2006-0734	2.3	Security Focus, Bugtraq ID: 16619, February 14, 2006
WebGUI WebGUI prior to 6.8.6-gamma.	A vulnerability has been reported in user account creation due to an error, which could let a remote malicious user bypass security restrictions. Updates available There is no exploit code required.	WebGUI User Creation Security Bypass CVE-2006-0680	Not Available	Secunia Advisory: SA18819, February 13, 2006
WHM Complete Solution WHMComplete Solution 2.2 & prior	A vulnerability has been reported in the Resellers Group, which could let a remote malicious user obtain sensitive information. The vendor has released WHMCompleteSolution 2.3 to address this issue. Please contact the vendor to obtain a fix. There is no exploit code required.	WHMComplete Solution Information Disclosure CVE-2006-0652	4.2	Security Focus, Bugtraq ID: 16560, February 9, 2006
WordPress WordPress 2.0	An HTML injection vulnerability has been reported in the Comment Post section due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. This vulnerability has been disputed by the vendor. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	WordPress HTML Injection CVE-2006-0733	2.3	Security Focus, Bugtraq ID: 16656, February 15, 2006
XMB Forum XMB Forum 1.9-1.9.3, 1.8, SP1-SP3	Multiple input validation vulnerabilities have been reported including Cross-SIte Scripting and SQL injection vulnerabilities due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML, script code, and SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	XMB Forum Multiple Input Validation	Not Available	Security Focus, Bugtraq ID: 16604, February 13, 2006

Xpdf Xpdf 3.01	A heap-based buffer overflow vulnerability has been reported when handling PDF splash images with overly large dimensions, which could let a remote malicious user execute arbitrary code. **Gentoo** **Fedora** **RedHat** **RedHat** **Ubuntu** **Debian** **Debian** **Debian** Currently we are not aware of any exploits for this vulnerability.	Xpdf PDF Splash Remote Buffer Overflow CVE-2006-0301	7	Secunia Advisory: SA18677, February 1, 2006 **Gentoo Linux Security Advisories, GLSA 200602-04 & GLSA 200602-05, February 12, 2006** **Fedora Update Notifications, FEDORA-2006-103, FEDORA-2006-104, & FEDORA-2006-105, February 10, 2006** **RedHat Security Advisories, RHSA-2006:0201-3 & RHSA-2006:0206-3, February 13, 2006** **Ubuntu Security Notice, USN-249-1, February 13, 2006** **Debian Security Advisories, DSA-971-1, DSA-972-1 & DSA-974-1, February 14 & 15, 2006**

[back to top]

Wireless Trends & Vulnerabilities

This section contains wireless vulnerabilities, articles, and malicious code that has been identified during the current reporting period.

- BlackBerry Enterprise Server Malformed Word Attachment Buffer Overflow: A corrupt Microsoft Word (.doc) file opened on a BlackBerry® wireless device could potentially provide a means to execute arbitrary code on the BlackBerry Attachment Service component of the BlackBerry Enterprise Server.
- Nokia Cell Phones Bluetooth Denials of Service: Two remote Denial of Service vulnerabilities were reported in Nokia cell phones in the Bluetooth stack.
- RSA turns everyday gadgets into security tokens: RSA Security is expected to announce a new user authentication method designed to replace traditional security tokens with cell phones, PDAs and other devices loaded with RSA's SecurID algorithm.
- Wi-Fi for dummies: The average user has no idea of the risks associated with public Wi-Fi hotspots. The article discusses some simple tips to keep network access secure.

[back to top]

General Trends

This section contains brief summaries and links to articles which discuss or present information pertinent to the cyber security community.

- Spyware remains rampant as Winamp exploited: According to a new study by the University of Washington, one in twenty executables on the Internet contain spyware. The study, which sampled more than 20 million Internet addresses, also found other disturbing trends. Among them: one in 62 Internet domains contains "drive-by download attacks," which try to force spyware onto the user's computer simply by visiting the website.
- Worms use Google to hunt for victims: According to McAfee's senior vice president for Risk Management, malware authors are increasingly starting to create digital pests that use the Google search engine to find their next victim. This automated vulnerability detection is the latest trend in a technique that is know as "Google hacking". Google hacking is a technique where online criminals use search engines to find sensitive information on the internet.
- Hackers look for holes in hosted applications: According to co-founder and chief hacking officer of enterprise security specialist at eEye, hosted web applications could soon become a target for e-criminals as they gain in popularity among enterprise users. Because hosted applications are run by a third party, research firms are not able to audit that software for vulnerabilities.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script),

trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
3	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.
4	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
5	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
6	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
7	Sober-Z	Win32 Worm	Stable	December 2005	This worm travels as an email attachment, forging the senders address, harvesting addresses from infected machines, and using its own mail engine. It further download code from the internet, installs into the registry, and reduces overall system security.
8	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
9	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
10	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.

Table updated February 13, 2006

[back to top]

Last updated February 16, 2006